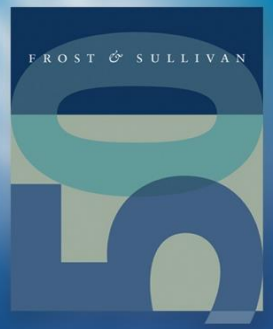
Artificial Intelligence (AI)-based Security Industry Guide

The need for AI-enhanced and automated security solutions for better threat prevention, detection & response

Cybersecurity Practice, Asia Pacific



PA74-74

September 2019

FROST & SULLIVAN

Contents

Executive Summary

Return to contents

Key Findings

- Artificial intelligence (AI) and machine learning (ML) have been adopted widely across industries over the years due to the multi-faceted benefits that the technologies bring about.
- AI and ML have been also increasingly adopted across industries, from healthcare, education, information & communication technologies (ICT), logistics, maritime, aviation, aerospace & defence, entertainment & gaming, etc.
- Particularly, AI and ML have been used widely in cybersecurity industries, by either bad guys and security communities, making the security landscape even more sophisticated. The AI-driven attacks are increasing in number and frequency, requiring security professionals to have more advanced, smart and automated technologies to combat these automated attacks.
- AI and ML have been used in all stages of cybersecurity to enable a smarter, more proactive and automated approach toward cyber defense, from threat prevention/ protection, threat detection/ threat hunting, threat response to predictive security strategy.
- Security startup companies are the most proactive in AI-security technologies with a great deal of number of AI-enabled security technologies introduced to the market. However, large traditional security companies have also beefed up their strategies to keep up with the trend of forging AI/ ML into their existing security solutions. Other trend can be observed is that start-up companies are increasingly acquired by these traditional security companies in the bid of strengthening their portfolios and capabilities.

Source: Frost & Sullivan

Artificial Intelligence Definition

Return to contents

Definition of Artificial Intelligence

- Artificial Intelligence is a set of technologies that enable machines to perform tasks normally requiring human intelligence, such as visual perception, image recognition and decision-making. Unlike the sci-fi movies that AI escape from human control, AI still under single domain phase. There are three levels of artificial intelligences and the AI development and applications so far are under Artificial Narrow Intelligence (ANI).

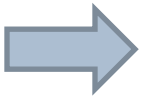
Artificial Narrow Intelligence (ANI)	Artificial General Intelligence (AGI)	Artificial Super Intelligence (ASI)
• Refers to machines that can display intelligence in limited and well-defined domains. • The machine is unable to transfer its abilities across domains • The industry has made significant progress in this area and continues to make groundbreaking innovations	• Refers to machines that can achieve human-like performance across more than one domain • These machines can also transfer their intelligence/abilities across domains. • It is still extremely complicated to realize such a system	• Refers to machines that have intelligence beyond humans across all domains, including creativity and social skills • These machines can transfer their intelligence/abilities across domains. • This category forms the basis of media hype and myths about AI systems.
Achievement of development: Plenty of ANI applications to serve particular issues/domains.	Achievement of development: No AGI development has been achieved at the moment.	Achievement of development: No ASI development has been achieved at the moment.

Source: Frost & Sullivan

Definition of Machine Learning and Deep Learning

Machine Learning (ML)

- An approach within ANI in which systems learn from and make predictions on data. **ML techniques are effective for situations involving limited data**, similar to human decision-making.
- The problem with traditional approaches is that they need a lot of training data to make a decision, making them poor in new situations.
- Machine Learning systems are different. **ML learn patterns within data**. These representations are more effective when applied to new and unknown data. This makes this approach ideal for predictions and for vision, language, and motion systems.

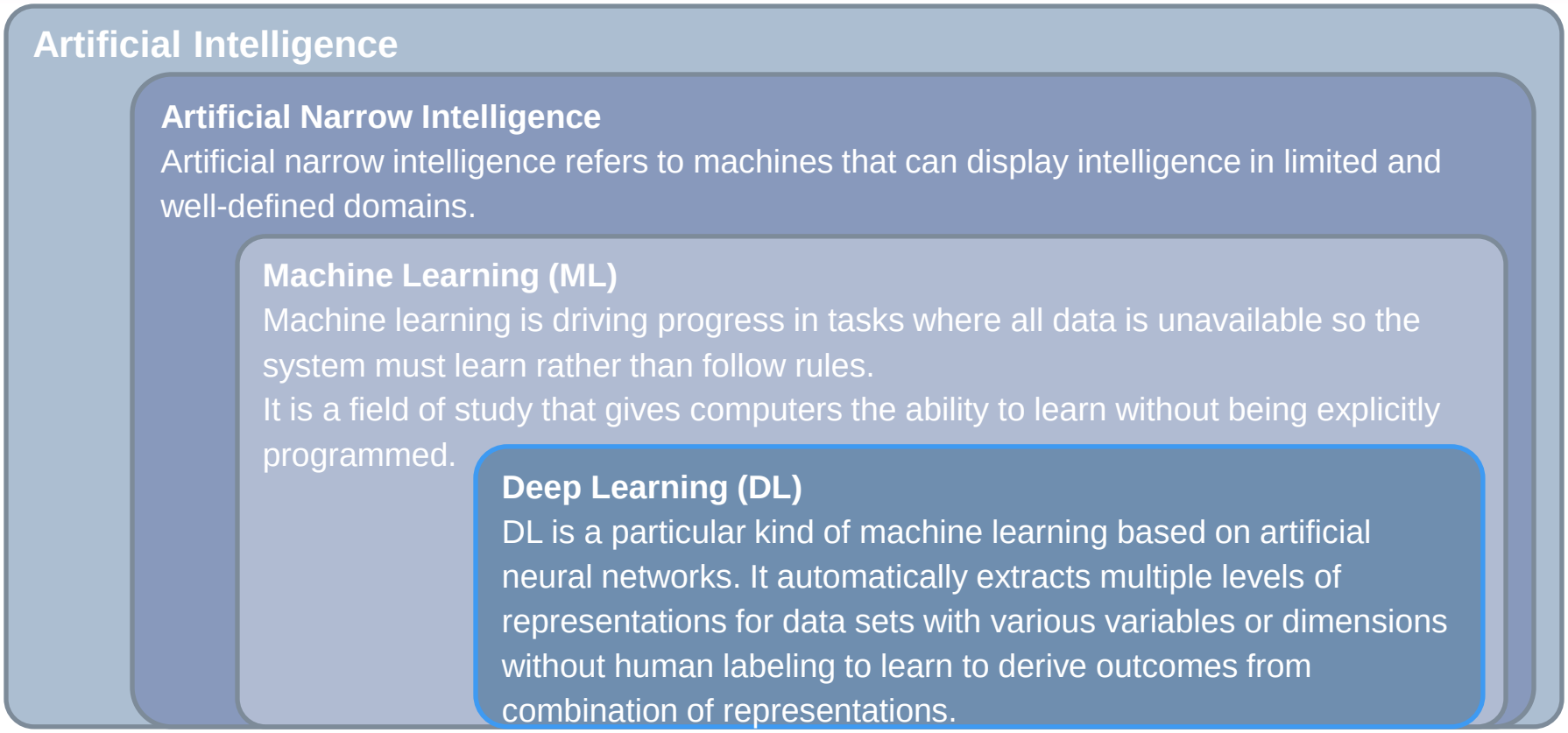


Deep Learning (DL)

- **Deep Learning is a class of machine learning (ML) algorithms** that use multiple layers of processing units that can **learn feature representations**.
- Deep learning techniques are 'deep' as they are based on massive artificial neural networks, much like how the human brain uses neurons.
- The input of each neuron is assigned a weight, where the final output is then determined by the total of these weights from the neurons.
- Example: Identifying a stop sign in foggy weather. The system might be 80% confident that the image is a stop sign, 13% confident it is a speed sign, and 7% confident that it is a kite. The entire network architecture will then tell the neural network whether it is right.

Source: Frost & Sullivan

AI, Machine Learning and Deep Learning



Overall, artificial intelligence is to enable the machines to perform human-like perception and decision-making. Machine learning is a subset of techniques to let machines to learn from data patterns without explicit instruction. Deep Learning is one of the most critical and the main AI techniques under discussion nowadays. DL is a class of ML algorithms that use multiple layers of processing units that can automatically extract and learn feature representations and infer the solution/prediction on new datasets.

Source: Frost & Sullivan

Deep Learning- A 2-part Process

Deep learning mainly comprises two specific tasks—training and inference of datasets. A new AI-enabled application will require to input data to conduct training and deploy the trained model to execute the inference workload when new data comes in.

Training

- Training is the first and compute-intensive phase for deep learning. Once the training datasets are available for the neural network, the machine will extract the features and assign a weight to determine whether it is correct or not and adjust the weight.
- The deep neural network is formed by several layers. An automatically assigned and examined weight of the previous layer will be assigned to be as the input of next layer.
- Every time input data into the network will help to examine the correctness of all weights in the hidden layers. The weights will be tuned over and over again until the final layer and the integration of layers that can match the correct final outcomes to form a trained model.
- Training is extremely compute-intensive. The trained model will lead us to part 2 – inference.

Inference

- The main point of inference is to create an efficient application that can retain the learning and apply it to data that it has never seen.
- Some examples include Apple's voice-activated assistant Siri, Facebook's image recognition in photo tagging, and Netflix's recommendation engines.
- When comes to inference, speed and latency becomes two key factors in determining the efficiency of this process, which leads to the crux of this study; understanding the capabilities of various processing processors in the market that allow for deep learning to be executed properly.

Deep Learning Algorithms to Deal With Diverse Tasks

CNN (Convolutional Neural Networks) – CNN excels at extracting high level feature representation and is design for image-oriented tasks such as image recognition, facial recognition, object detection and can also apply to different types of classifications, anomaly detections

RNN (Recurrent Neural Networks) – RNN is particularly applied to sequential or contextual problems such as sequence prediction and context, text or conversational processing (Natural language understanding)

GAN (Generative Adversarial Networks) – GAN applies the imitation and simulation technique to produce new dataset from the original data. For example, the machine can create a new face image, a voice, a video clip etc which do not exist, hard to collect or rarely happened repeatedly. GAN help machine to be self-sufficient on both populating new dataset and providing better reaction to unexpected or unknown situations based on more simulated scenarios.

For many circumstances, developers adopt and integrate different types of networks to address issues with multiple dimensions.

Source: Frost & Sullivan

AI – Diligent and Resources to Support Applications

AI is actually not a new term. However, only in these few years, a series of investment and supporting resources are making AI-enabled applications relatively efficient and feasible.
Increasing amount of companies are announcing the involvement of developing and providing AI services or integrating AI techniques into their businesses/products.
In fact, there are several fundamental AI enablers altogether to deliver the final applications. The key enablers include:

1) Computing power - include processors such as CPU, GPU, FPGA to deliver computing power particularly for deep learning training and inference workloads

2) Data - processable structured or unstructured datasets

3) Framework, library, and diverse algorithms to support tasks. Many of framework and models are now open-sourced to developers.

Increasing amount of technology companies, start-ups and enterprises are involving in the AI-enabled applications but it is still challenging to depict a clear AI business ecosystem so far.
Lastly, although prion to neglect, time is a critical and necessary factor in not only processing the data but the initial and continuous fine-tune of AI models. AI-enabled solutions require “training” period to learn and adjust to deliver results.

Source: Frost & Sullivan

AI Adoption Trends

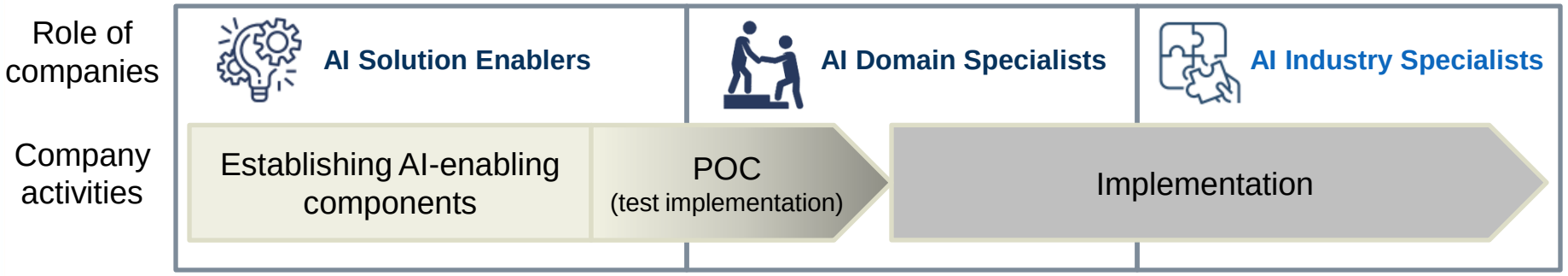
Return to contents

AI Industry Specialists develop Vertical Applications

Frost & Sullivan defines the roles of AI service providers to three types from different standing points and activities executed. The roles are not mutually exclusive. The role a company played might change and coexist along the development of technologies and transformation of business.

The three types of AI service providers are **AI Solution Enablers, AI Domain Specialist and AI Industry Specialist**.

AI Solution Enablers are companies which can provide individual essential AI components. **AI Domain Specialists** focus on specific AI functions such as Natural Language Understanding for intelligent chat-bot, Computer Vision for object recognition. **AI Industry Specialists** is the last type of key player. These players focus on industry or vertical solutions with exclusive data, domain know-how or proprietary models to deal with particular industry issues for example, medical diagnostic, autonomous driving, smart retailing, cyber security malware mutation detection and prediction etc. With the advantage on domain knowledge and experience, AI Industry Specialist can input data to build proprietary AI model or retrain AI models with exclusive datasets. AI Industry Specialists provide more advanced, efficient or personalized solutions and services to clients. So far, there are still limited AI Industry Specialists provide commercialized services/ products to share with or be adopted by external users, particularly in APAC. We expect to see increasing development and adoption moving forward.



Source: Frost & Sullivan

AI at the Edge Increases Cyber Security Risks

Follow the AI discussion, developing AI models requires huge amount of data and computing power to support the workloads to unlock AI capabilities. Data center support compute-intensive workload and data storage.

Nowadays, with proliferation of IoT smart devices to support certain level of data processing and analysis capabilities, many solutions need to find ways to strike a balance between what needs to be at the edge and core (the data center).

Edge computing enables data to be pre-processed and filtered at the edge. This reduces the strain on networking and reinforces security. Analysis at the edge also enables better fusion of data to provide situational analysis and context. The edge is getting increasingly important. However, on the other hand, with increasing adoption of edge devices, it also rise identity authentication, network access control and cyber security update issues on edge devices. Developers needs to be aware of the potential risk and well-prepare and design the services to address the relevant potential risks.

Advantage of AI and IoT technology at the edge

- Time-critical, closer to real-time
- Pre-process and filter data
- Data security (transmit only necessary information)
- Spontaneous analysis and respond

Advantage of AI and IoT technology to data center

- Computing power
- Complex data processing
- Data storage

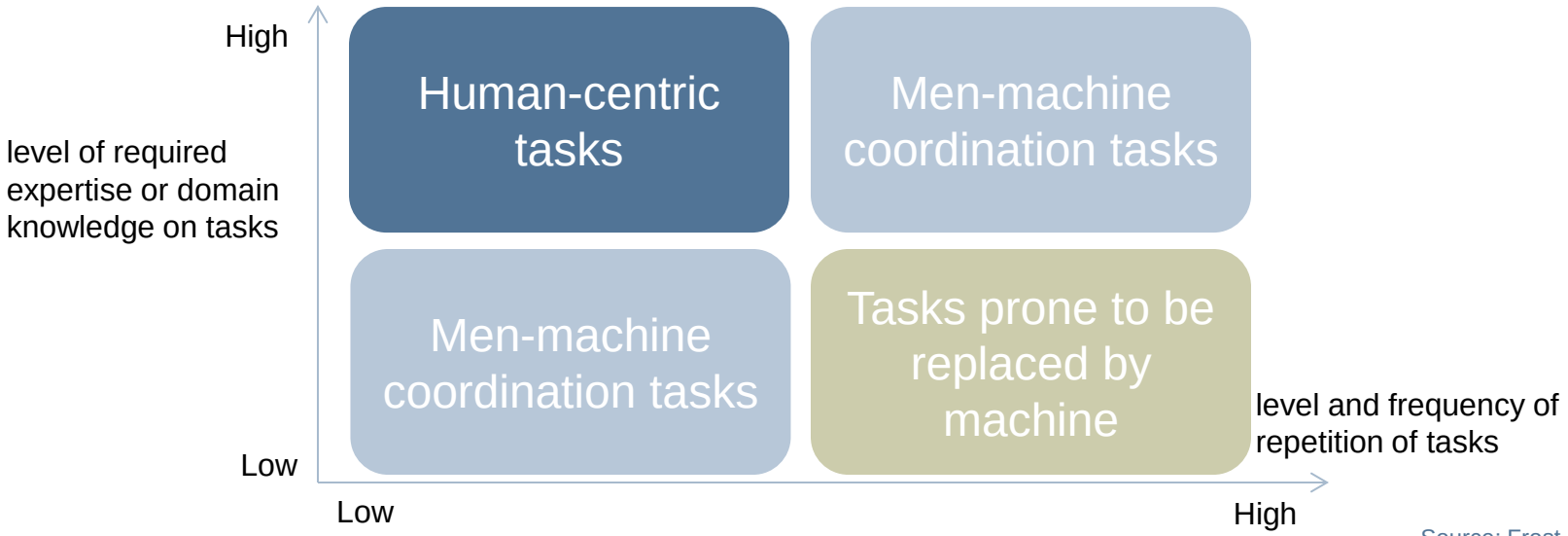
Source: Frost & Sullivan

Increasing Human-machine Coordination

The advantages of artificial intelligence on dealing with massive amount of information and complex issues with designed algorithms increase the added-value, productivity and reduce potential costs to users. On the other hand, AI-enabled applications also raises the issue of replacement and reskill needs to employees.

Based on different level and frequency of repetition on tasks and take the level of required expertise or domain knowledge on tasks into consideration, only a fraction of tasks will be fully replaced by machine or fully executed by human. Majority tasks require human to cooperate with AI-enabled technologies.

In the future of work with AI-enabled technologies, there will be more men-machine coordination. AI-enabled applications assist employees to better deliver the services and enhance efficiency. Enterprises should estimate the potential benefit and impact to embrace the journey of digital transformation.



Source: Frost & Sullivan

AI-based Security Solution Profiles

Return to contents

Market Landscape

AI/ ML has been increasingly developed by security companies to strengthen their competitiveness. Most of them now have been in the midst of developing their own AI/ ML algorithm to empower their security products, either in certain product or all of product lines. For example, Cisco Systems is developing its AI/ ML to empower its intent-based networking and datacenter security solutions. Fortinet has been integrated AI/ML into its Fortiweb solution to fight against web-based application threats. Symantec has recently added AI/ ML capabilities to enhance its endpoint security protection wit its AI-powered Targeted Attack Analytics (TAA) for incident response. While most of security giants are just embedding AI/ML into some certain security products, we have seen increasing number of companies that have been developing the AI/ML-driven security products, which have gained greater traction in the market.

There are hundreds of such companies now in the market with different capabilities and focused areas, from application-centric protection, AEDR, to security analytics platform. In this report, we profile those companies that are AI/ML-driven and AI/ML-centric cybersecurity companies. In the next update, we would like to include more companies that have AI/ML-driven products that have been largely adopted by enterprises.

Companies that are profiled in this report include:

Balbix, CROWDSTRIKE, DARKTRACE, 安恒信息 DAS-security 安全中国, eSENTIRE, PALADION BETTER SECURITY OUTCOMES, REAQTA, seceon, SHAPE SECURITY

Source: Frost & Sullivan

Seceon

Country of Origin	Solution Name	Solution Type	Security Category	Commercial Form Factor
US	Seceon aiSIEM	SIEM	Detection & SOAR	On-premises, Cloud and Hybrid

Solution Overview:

- Seceon aiSIEM is a platform that ingests raw streaming data, such as logs, network flows and identities from OS, Apps, devices, network infrastructure and cloud infrastructure including SaaS, PaaS, IaaS, IoTs and IIoTs. It consumes **logs** from all devices, OS, Apps and Services in the ecosystem (on-premise, cloud); f**lows**, such as, NetFlow, IPFix, sFlow, jFlow from network infrastructure, and subscribes to **identity** management infrastructure, such as, Microsoft® Windows® Active Directory™ service, LDAP, DNS, DHCP, Azure AD, etc. The platform includes functionalities of traditional SIEM with the addition of other security operation functionalities, such as SOAR, user and entity behavioral analytics (UEBA), NBAD, NTA, IDS, threat intelligence feeds for correlation and, particularly the advanced machine learning (ML)/ artificial intelligence (AI).
- The ML/AI enables the platform to generate contextual & situational alerts and actionable intelligence. It also provides improved accuracy of threat indicators for better security operations, i.e., proactive threat detection and automated response by communicating with other security solutions, such as, firewall, IPS, identity management infrastructure, email security and web security, EDR, etc. The AI engine automates the analysis & correlation to minimize the false positives and reducing SOC overheads.

Key Features:

- ***Behavioral analytics & predictive modeling:*** It uses ML for unsupervised and supervised learning in real-time, to analyze data collected from different sources for accurate and proactive detection of threats, including zero-day malware and insider attacks, and to facilitate prediction based on user behaviors and big data analytics.
- ***Contextual real-time alerts and automated threat response:*** The platform provides contextual real time alerts and actionable insights by leveraging the capabilities of automated analysis and advance correlation to enable security teams to respond to the threats fast and effectively. It also supports automated response based on the policies being applied.
- ***Dynamic threat models:*** The platform automates the rule creation process to detect the threats based on the threat indicators. The threat models are preconfigured and able to adjust dynamically by self-learning and adapting over the time to reduce the alert volume by surfacing threats that matter and helping the SOC team to address prioritized threats/ incidents.

Seceon

Key Differentiators:

- ***Reduce the MTTD (Mean time to detect) and MTTR (Mean time to respond):*** By using advanced ML/ AI engine that process a large amount of raw data, the platform is able to perform deep data analysis dynamically to help identify threats in real-time more effectively, reducing the MTTD and MTTR. The platform helps reduce the operation complexity by using the dynamic threat models and user behavioral analysis to eliminate the process of manual rule writing. The automated threat analysis and correlation AI engine can generate the actionable alerts that helps security team to increase the threat detection accuracy, reducing false positive alerts to respond faster to the identified threats/ incidents, which in the end enables organization to reduce more than 80% of security operation costs (as per the company's announcement). Especially, when the platform is adopted by an MSSP, it will help increase their security operations to respond faster to their client requests as one analyst is able to handle around 500 customers at the same time.
- ***Dynamic threat models with UEBA and advanced machine learning/ AI:*** The platform is integrated with advanced analytics technologies such as UEBA, threat intelligence feeds, anomaly detection algorithm for signature-less threat detection without the need to create rules, which helps increase the threat detection capabilities and automate the process with the minimum requirements for human intervention.
- ***Continuous compliance and monitoring:*** aiSIEM provides reports for regulatory compliance, including HIPAA, PCI, NIST, FINRA, GDPR and investigation support, enabling organizations to comply with the standards and also continuously monitor and report against this compliance. The reports can be generated on demand any time.
- ***Comprehensive Visualization:*** Seceon ingests raw streaming data - logs from all devices, OS, apps and services in the ecosystem (on-premise, cloud or both), flows from network infrastructure - and subscribes to identity management infrastructure. It enriches the extracted data to provide real-time comprehensive visibility of all assets and their interactions.

Business Overview :

- Seceon's main business is in the US with a significant number of clients from service providers and mid-to-large enterprises that run a security operation center (SOC). The company is rapidly expanding its presence in other regions, including Europe and Asia Pacific with sales offices in the UK, Japan and India.

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan
3211 Scott Blvd, Suite 203
Santa Clara, CA 95054

Appendix

Return to contents

Final Words

The adoption of AI/ ML in cybersecrutiy has increasingly changed the approach toward security strategy as a whole as well as security operation at the tactic level. From the tactical security operation perspective, AI/ ML is empowered to help organizations to prevent, detect and respond to threats faster and more accurately with the minimum of human involvement.

This is changing the approach to security planning among organizations as many of them are likely to leveraging on AI/ ML to restructure the whole security strategy by driving the security operation automation and reducing the cost of other technologies, people and processes.

However, it is worth noting that AI/ ML is still at the early stage and the technology is unable to replace the human factor at the moment. AI/ ML can only be used to facilitate the decision making process but not to replace it. The outcomes of AI/ ML analytics technologies is sill greatly reliant on the input data it is fed and how the algorithm is set. In other word, the results of AI/ ML analysis still requires human analysis, evaluation and experience so that the decision is accurately made based on these AI/ ML generated results.

Secondly, as AI/ ML is also a software that can also be compromised by other software or AI program. This will represent a severe consequences as the compromise can go undetected for a long time before being detected by either security software or human.

As a result, AI/ ML systems should be adopted along with a holistic security strategy where technologies, human and processes are adequately invested. AI/ ML system will become an important assistance to the overall security strategy and daily operation, which can serve different purposes, either to increase security operation efficiency or to reduce costs, or both.

Source: Frost & Sullivan

The Frost & Sullivan Story

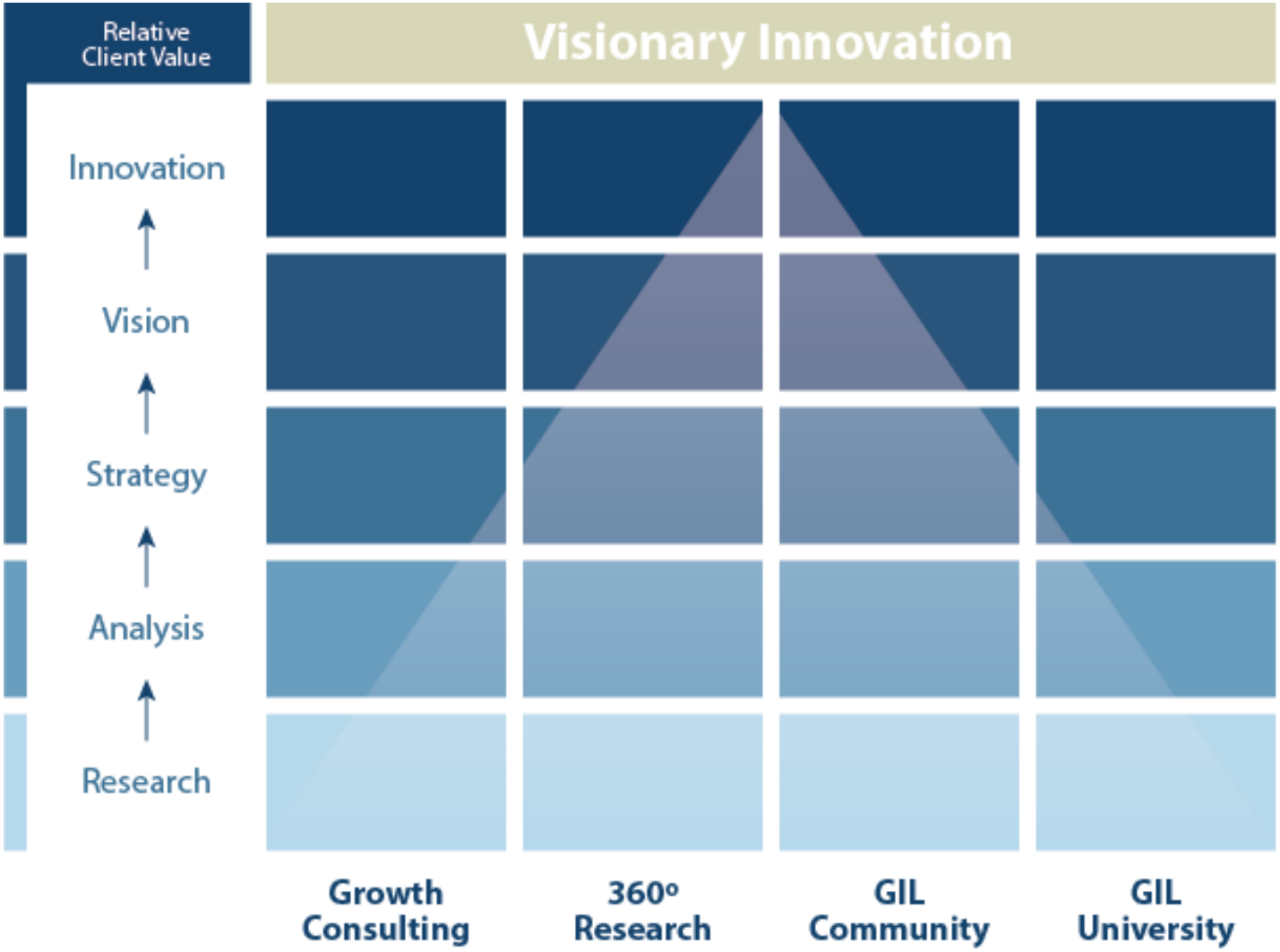
The Journey to Visionary Innovation

Return to contents

The Frost & Sullivan Story

Value Proposition: Future of Your Company & Career

Our 4 Services Drive Each Level of Relative Client Value



Global Perspective

40+ Offices Monitoring for Opportunities and Challenges

Industry Convergence

Comprehensive Industry Coverage Sparks Innovation Opportunities

Aerospace & Defense

Measurement & Instrumentation

Consumer Technologies

Information & Communication Technologies

Automotive Transportation & Logistics

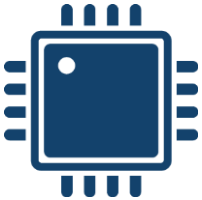
Energy & Power Systems

Environment & Building Technologies

Healthcare

Minerals & Mining

Chemicals, Materials & Food



Electronics & Security

Industrial Automation & Process Control

360º Research Perspective

Integration of 7 Research Methodologies Provides Visionary Perspective

Implementation Excellence

Leveraging Career Best Practices to Maximize Impact

Our Blue Ocean Strategy

Collaboration, Research and Vision Sparks Innovation